

Headlines

- Enabling large-scale IoT – Arm Pelion IoT Platform and Intel Secure Device Onboard
- Adlink Adds Foghorn Edge Intelligence to IoT Digital eXperiments as-a-Service
- 5 IoT Energy-Harvesting Options Stand Out “in the Field”
- Telia Norway connects bins in country's biggest NB-IoT contract



Crypto-Authentication

Protect IP and Deploy
Secured Connected Systems
with Microchip's New
CryptoAuthentication™ Device
ATECC608A



In this is Edition

- COVER STORY:

Protect IP and Deploy Secured Connected Systems with Microchip's New CryptoAuthentication™ Device ATECC608A

- ADLINK Adds Foghorn Edge Intelligence to IoT Digital eXperiments as-a-Service (DXS)

Alliance enables high-fidelity, real-time analytics and edge-based machine learning in ADLINK's IoT experiments

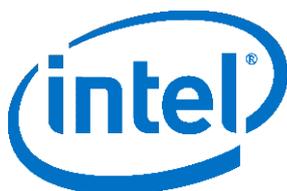
- Telia Norway connects bins in country's biggest NB-IoT contract

Telia Company is bringing waste disposal into the Internet of Things after signing what it is claiming is Norway's largest NB-IoT contract



- Enabling large-scale IoT – Arm Pelion IoT Platform and Intel Secure Device Onboard

Fulfilling Pelion's "Any device, any data, any cloud" vision



- WinSystems Introduces Pico-ITX Single Board Computer With Ideal Functionality for Embedded Industrial IoT Applications

- Entrust Datacard and ADLINK Partner to Enable Trust at the Edge

Technology partnership promotes secure-by-design adoption of the Internet of Things

- These 5 IoT Energy-Harvesting Options Stand Out "in the Field"

- Fundamentals of Power - Welcome to the Power Design Center of Texas Instruments

Over 25 applications notes FREE for direct download

Daniel Dierickx
CEO & co-Founder
at e2mos
Acting Chief Editor



*Over 3 decades
Chips & Embedded
Systems Market Expertise*

Dear Reader,

Here is your free copy of **IoT World**, one of our five magazines

Your benefits:

- Selected subjects
- Easy reading
- Many direct links for more
- Efficient time saving
- FREE Worldwide

FREE Subscription

Click on the logos below



Editor/Publisher: **e2mos**

WEB: www.e2mos.com

Contact: mgt@e2mos.com

Our SERVICES Worldwide

- New Customers Discovery and meeting setup
- Coaching - Filling the gaps Upgrade your Customer Database
- Massive Global Market Reach with our PREMIER Database

Take a look at
www.e2mos.com

ADLINK Adds Foghorn Edge Intelligence to IoT Digital eXperiments as-a-Service (DXS)

Alliance enables high-fidelity, real-time analytics and edge-based machine learning in ADLINK's IoT experiments

San Jose | 12 Jul 2018

ADLINK Technology, a global provider of leading edge computing solutions, has partnered with FogHorn Systems, a leading developer of software for industrial and commercial Internet of Things (IIoT) solutions, to bring edge intelligence to ADLINK's groundbreaking [DXS IoT digital experiments as-a-service](#). DXS enables the testing of potential IoT-based endeavors to determine the viability of possible solutions with none of the upfront costs and risk associated with a full solution commitment.

Full IoT solutions conventionally require significant upfront investment, despite, according to industry studies, success rates for such projects only reaching 26%. The vendor-agnostic DXS provides all the resources required to get digital experiments up and running—including pre-validated hardware, client asset connection, data movement consolidation to bridge the IT/OT gap, enterprise sharing, endpoint management, and field and professional services—without associated upfront costs.

"ADLINK DXS enables industrial organizations to think big, start small and work fast when integrating IoT-based functionality within new business models or processes," said Andy Penfold, director of offering management, ADLINK IoT Solutions and Technology. "It's very clear an edge-to-cloud approach will emerge as a primary design principle in IIoT production deployments, so adding the leading provider of edge intelligence into the DXS creates, in our opinion, the most advanced testing ground available for IIoT projects."

[FogHorn's Lightning™](#) product portfolio brings an innovative dimension to IIoT by embedding edge intelligence as close as possible to the source of streaming sensor data. The FogHorn platform is a highly compact, advanced and feature-rich edge intelligence solution that delivers unprecedented low latency for onsite data processing and real-time analytics in addition to its machine learning (ML) and artificial intelligence capabilities. FogHorn's cloud-agnostic approach offers a fully-integrated, closed-loop edge-to-cloud solution, maximizing real-time insights and rapidly iterating ML models to adjust to constantly changing operating conditions.

FogHorn Lightning offers ADLINK DXS customers several benefits, including:

- Real-time, CEP-based streaming analytics enabling faster actionable insights for greater operating efficiencies
- Edge-to-cloud iterative machine learning for higher quality predictive insights
- Radically lower data persistence and transport requirements by processing live data at the source
- Enhanced security posture by eliminates the need to transmit critical OT data across networks

"ADLINK is meeting a critical need in the market today with its DXS offering, giving organizations the tools and expertise to model multiple IIoT use cases with little risk or cost," said Kevin Duffy, vice president of business development at FogHorn. "FogHorn is a natural extension of this initiative to bring the technical and economic benefits of edge intelligence into the modeling of IIoT projects. We're very excited to be working with ADLINK."

ADLINK DXS provides organizations with all the benefits of digital experimentation and enables rapid evaluation of experiments, resulting in blueprints that can be replicated, scaled up and rolled out. The approaches each project individually to determine which areas are likely to be affected by the solution, from ground-level operations to admin and resource allocation. Each digital experiment is defined at the intersection of people, places and affected assets, where most value can be created.

"Our service leverages technologies through all layers of the required hardware, software and network stacks to create viable, scalable and secure IoT solutions," Penfold added. "These solutions span not only capabilities from ADLINK, but also from partners throughout our ecosystem, and are therefore agnostic in nature."

Click [here](#) for more information.

Protect IP and Deploy Secured Connected Systems with Microchip's New CryptoAuthentication™ Device ATECC608A



Features:

- Cryptographic co-processor with secure hardware-based key storage
- Protected storage for up to 16 Keys, certificates or data
- ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman
- NIST standard P256 elliptic curve support
- SHA-256 & HMAC hash including off-chip context save/restore
- AES-128: encrypt/decrypt, galois field multiply for GCM

[View More](#)



Device Overview

The Microchip ATECC608A integrates ECDH (Elliptic Curve Diffie Hellman) security protocol an ultra-secure method to provide key agreement for encryption/decryption, along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication for the Internet of Things (IoT) market including home automation, industrial networking, medical, as well as accessories and consumables authentication and more. In addition, the ATECC608A offer an integrated AES hardware accelerator strengthening hardware based security for LoRaWAN applications and enable secure boot capabilities for very small microcontrollers.

The ATECC608A is a secure element from the Microchip CryptoAuthentication™ portfolio with advanced Elliptic Curve Cryptography (ECC) capabilities. With ECDH and ECDSA being built right in, this device is ideal for the rapidly growing IoT market by easily supplying the full range of security such as confidentiality, data integrity, and authentication to systems with MCU or MPUs running encryption/decryption algorithms. Similar to all Microchip CryptoAuthentication products, the new ATECC608A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which eliminate potential backdoors linked to software weaknesses.

The device is agnostic of any microprocessor (MPU) or microcontroller (MCU) and compatible with Microchip AVR/ARM MCUs or MPUs. As with all CryptoAuthentication devices, the ATECC608A delivers extremely low-power consumption, requires only a single GPIO over a wide voltage range, and has a tiny form factor making it ideal for a variety of applications that require longer battery life and flexible form factors.

Take a look at the various use cases including :

- Cloud authentication for [AWS IoT](#)
- Cloud Authentication for [Google Cloud IoT Core](#)
- [Secure Boot](#) implementation with an ATSAMD21 Cortex-M0+

View Datasheet [CLICK HERE](#)

Telia Norway connects bins in country's biggest NB-IoT contract

Telia Company is bringing waste disposal into the Internet of Things after signing what it is claiming is Norway's largest NB-IoT contract.

MOBILE EUROPE | 02-Oct-2018



The operator has signed a three year deal with waste disposal container tracking company StalkIT, spanning 100,000 connected devices.

It has developed a service that gives waste management companies the ability to track the location and status of their containers.

Einar Aaland, Chief Product Officer at StalkIT, said: "All our customers need to do now is to mount the tracking device on their containers and switch it on. Our tracking service will provide them with a complete overview of where the containers are and what status they have, and the investment will provide quick returns because processes can be automated and waste can be reduced."

Jon Christian Hillestad, Vice President Enterprise at Telia Norway, said: "We are proud to have a wide-ranging agreement with an entrepreneurial company with great ambitions. It is very exciting to see our pilot project from this winter going commercial with the potential to expand beyond the Norwegian borders."

It launched its NB-IoT network earlier this year and has recently completed nationwide coverage.

Across all of parent Telia Company's opcos, the operator has held some of the quirkiest trials of the technology, exploring how NB-IoT can be used in [postboxes in Finland](#), [construction in Norway](#), and [tracking athletes in an Ironman competition](#).

While operators have been flocking to NB-IoT to offer new kinds of services to customers, [a note of caution was sounded by ABI Research in July](#), when it said it and fellow cellular technology LTE-M would continue to face pressure from unlicensed technology such as LoRa and Sigfox.

ARM Press Release, see below
Source: [Click Here](#)

Intel Press Release
Source: [Click Here](#)

Enabling large-scale IoT – Arm Pelion IoT Platform and Intel Secure Device Onboard

Fulfilling Pelion's "Any device, any data, any cloud" vision

By [Bill Curtis](#), Arm IoT Strategy | 18-Oct-2018 --

The Internet of Things (IoT) is rapidly transitioning from early deployments into a new phase of aggressive growth that we expect will result in deployment of one trillion connected devices by 2035. However, this is only achievable if the IoT industry transitions to more open and scalable methods for automatically onboarding onto cloud application platforms. Earlier this year, Arm and Intel began exploring opportunities for integrating our respective device provisioning systems with a goal of accelerating this process. Intel® Secure Device Onboard (Intel® SDO) is a dedicated onboarding service that provides a dynamic "late binding" approach to provisioning where the device owner's target cloud application and access credentials can be assigned at any point in the supply chain. Arm's Pelion Device Management service automates both device onboarding and provisioning to any cloud application layer and manages devices through their lifecycles. The combination of these two solutions adds more flexibility to Pelion's supply chain enablement and expands device coverage to include Intel Architecture (x86) platforms.

This week, Arm and Intel are demonstrating a prototype of an integrated Pelion-Intel SDO provisioning system at [Arm TechCon](#) and [IoT Solutions World Congress](#). This demo shows deployment-time credential assignment for both Arm and Intel Architecture devices. Intel SDO manages device credentials and specifies the application layer, and The Pelion IoT Platform provisions the device, manages it, and connects it with the selected application layer. This integrated demo is true to Arm's "any device, any cloud" vision for the Pelion IoT Platform.

You can read more about the [full Arm Pelion announcement on our Newsroom](#).

Zero touch

Today, many IoT devices are delivered to customers in a state that requires manual intervention to provision them for secure connection with application services. For instance, a skilled technician might have to type in or scan the identity of a device or in some cases cut-and-paste key material between devices and services. Clearly, this time consuming and error-prone process is limiting IoT growth. Ideally, IoT devices are installed automatically by simply powering them up and providing access to a network. Each device then contacts its provisioning service, identifies itself, and exchanges authentication information so that the device can trust the service and the service can trust the device. The provisioning service then makes the final connection between the device and the application service. This technique is sometimes called "zero touch" because the whole onboarding process can be directed without physical access to the device. Zero touch is available today from the [Pelion Device Management service](#).

... to next page

Enabling large-scale IoT – Arm Pelion IoT Platform and Intel Secure Device Onboard

... from previous page

Late binding

Although zero touch is a big improvement over manual configuration, the technique can create a big scaling barrier of its own. If deployment-specific credentials must be configured during device manufacturing then each such configuration is, in effect, a unique manufacturing SKU. These individual SKUs must be managed as unique products through IoT supply chains (manufacturing, distribution, systems integration, installation, etc.). It would be far more efficient to manufacture IoT devices “by the truckload” that are all identical and then customize them for specific deployments late in the supply chain. That customization includes specifying the application service, providing authentication credentials, and in some cases loading new firmware components. Specifying this information at any point in the supply chain is referred to as “late binding” because devices can be bound to applications and cloud frameworks at any time, often just prior to deployment. Arm Pelion Device Management and Intel SDO provide late binding today. Application services and credentials can be specified at any time prior to installation (late binding) and devices can be onboarded automatically (zero touch).

Pelion Device Management and SDO

Intel® SDO complements Pelion by providing formal methods for transferring “ownership” of a device from one party to another. Device ownership is represented by a “digital ownership voucher” which is chain of nested security credentials that identify both the device and its current owner. This digital voucher may also contain deployment credentials such as the device's application service – Pelion, for instance – as well as connectivity parameters and other data. The digital voucher is like a ledger that is securely passed from one company to another as a device moves through an IoT supply chain. Pelion and other IoT frameworks already have ways of doing this kind of thing but Intel SDO adds value in two ways. First, transfer of ownership is secure and explicit because each owner signs the digital voucher over to the next one in the supply chain. There is no ambiguity about who owns the device, where it came from, or who set the onboarding parameters. Second, Intel SDO is not dependent on any specific platform architecture or operating system. In other words, Intel SDO provides an alternate method for specifying device onboarding parameters that is both secure and device independent.

Intel SDO enables late binding of device and cloud credentials, but it is not an IoT device management system. It manages the ownership and onboarding credentials and delivers them during the onboarding process. Combining Intel SDO with Pelion Device Management provides a complete solution to zero-touch onboarding with late binding of credentials and cloud-independent hosting. Together, Arm's Pelion Device Management and Intel SDO's onboarding service allow organizations to manufacture devices without any prior knowledge of customer-specific onboarding credentials or even which application framework the end user will choose, thereby shifting the industry from siloed supply chains to a harmonized framework for the design and sourcing of secure, connectable devices. Any IoT device, [Cortex-M](#), [Cortex-A](#), or Intel Architecture based, can be manufactured without knowledge of who will own it, how it will travel through a supply chain, or which cloud service will ultimately use it, and it will still automatically appear on the correct cloud service using the correct customer account. This is especially beneficial for organizations that have several device types based on different technologies because it enables onboarding credentials to be set the same way for every type of device and at any point in the supply chain.

Arm partner benefits

For silicon providers and device OEMs, the combination of Intel SDO and Pelion means that a single SKU can now serve the needs of multiple customers and applications. This is because application services and user assignments can be made at any point in the supply chain, not just in manufacturing. Sales channel velocity and time-to-market are also improved because customers can separate device procurement decisions from cloud deployment strategies.

System Integrators and IoT application providers benefit because they can receive ownership of a device, add value, optionally specify which cloud application to use, and then pass it along to the end-user or the next node in the IoT supply chain with the device chain of trust intact. This is truly transformational because it enables more companies to add value to IoT devices without compromising security.

“Any device, any cloud” benefits end-users because secure device onboarding, management, and connectivity are no longer bound to specific device architectures, applications, or cloud frameworks. This flexibility reduces cost and business risk.

Conclusion

The combination of Arm Pelion Device Management and Intel® Secure Device Onboard eliminates key IoT scaling barriers by providing platform-agnostic onboarding (any device – Arm-based and x86), cloud-agnostic deployments (any cloud), and improved supply chain efficiency (lower cost and risk). Over the next few months, Arm and Intel will be working with partners to put this new technology into commercial service.

[Interested in learning more about Arm Pelion Device Management?](#)

WinSystems Introduces Pico-ITX Single Board Computer With Ideal Functionality for Embedded Industrial IoT Applications



Rugged ITX-P-3800 design packs fanless performance into miniscule form factor; embedded SBC offers industrial connectors and -20°C to +70°C operating temperature range

ARLINGTON, Texas – October 30, 2018 – Industrial embedded computer leader WinSystems today announced its Intel E-3800 processor-based computing platform in the Pico-ITX form factor. Measuring a mere 3.9 inches by 2.8 inches (100 mm by 72 mm), the ITX-P-3800 delivers low-power performance, endurance, and versatility. The proven design of this rugged single board computer (SBC) accelerates time to market for new products while assuring that they will perform reliably in critical applications for many years – even under harsh operating conditions. Equally important, it gives embedded and industrial IoT designers the flexibility to create unique designs via easy-to-use expansion and configuration settings.

Features

- PICO-ITX Form Factor (102mm x 73mm)
- Intel® ATOM E3845/E3825 Processor
- Up to 4GB DDR3-LV RAM
- Dual Gigabit Ethernet
- 4x USB 2.0 and 1x USB 3.1 Gen 1
- Two 10/100/1000 Mbps Ethernet Ports
- 4x Serial Ports
- 4x Digital Inputs and 4x Digital Outputs
- One Full PCIe Mini Card/mSATA slot and One Half PCIe Mini Card slot
- Wide Range Power Input (+9 to +36V DC)
- -20°C to +70°C Operational Temperature



“The ITX-P-3800 was specifically designed to provide maximum flexibility, functionality and durability within an extremely small form factor,” said Technical Sales Director George Hilliard. “Beyond impressive fanless processing power and an optimum mix of features, its header-based connectors allow these SBCs to easily support diverse packaging solutions, including use within tight enclosures.”

WinSystems' innovative Pico-ITX SBC provides a complete system using the latest technology. It incorporates the most frequently used functionality for Industrial IoT applications and Human Machine Interface (HMI) displays and withstands operating temperatures from -20°F to +70°F. The ITX-P-3800 also offers the performance required to run Windows 10 IoT and Linux operating systems and enables extended life cycle solutions for energy management, medical and unmanned vehicle designs.

ITX-P-3800 single board computers include dual Ethernet and four USB channels, and accommodate a wide range of DC input power: + 9V to + 36V. They combine powerful Intel E3800 processors with a functional I/O set including four RS-232 serial ports plus a Mini-PCIe connector for easy expansion. The smaller header-based connectors allow the SBC to be used within a small box or container.

REDUCE PRODUCT-DEVELOPMENT RISK AND TIME TO MARKET

By relying on WinSystems' expertise in embedded computer design and manufacturing, customers can be confident their highly reliable products are built on the right computer system. The company's single board computers and embedded systems are backed by world-class customer service and responsive technical support from knowledgeable application engineers at every step of the process.

ABOUT WINSYSTEMS

Founded in 1982, WinSystems, Inc. designs and manufactures embedded single board computers (SBCs), I/O modules, and panel PCs that operate over extended temperatures. These products are engineered for demanding requirements and harsh environments, including industrial IoT, industrial automation/ control, transportation management, energy management, Mil-COTS, medical, digital signage and communications applications. For more information, contact Technical Sales Director George Hilliard at sales@winsystems.com or +1-817-274-7553, ext. 125. www.WinSystems.com

Entrust Datacard and ADLINK Partner to Enable Trust at the Edge



Technology partnership promotes secure-by-design adoption of the Internet of Things

Minneapolis | 27-Sep-2018



Entrust Datacard, a leading provider of trusted identity and secure transaction technology solutions, and ADLINK Technology, Inc., a global provider of Leading Edge Computing solutions, today announced a new partnership that solves one of the most significant barriers to adoption of the Internet-of-Things (IoT): Security. This collaboration will create an Industrial IoT (IIoT) security model, enabling secure communication for data streams throughout the entire IIoT value chain – from manufacturing and applications, to endpoints and edge devices.

The partnership will integrate Entrust Datacard's ioTrust™ Security Solution into ADLINK's Vortex Edge™ solution. The enhanced joint solution can quickly operationalize systems and things securely for every endpoint, application, container and data stream. The integration will ultimately provide customers with established and secure trusted identities across their IIoT ecosystems from the discovery phase to full roll out of their IIoT deployments.

This joint solution will also be included as part of ADLINK's Digital Experiments as-a-Service (DXS), which has been designed to test and assess the effectiveness of an IIoT solution design, strategy, organizational compatibility, and financial return. Organizations looking to develop secure by design Edge IIoT projects can now proceed with confidence knowing that they can try a number of scenarios without large upfront costs, as DXS is typically offered as a three-month engagement including access to a comprehensive suite of Vortex Edge™ microservices supported by an ecosystem of market leading partners, which negates the need for building bespoke complex systems.

"The IIoT is advancing rapidly and customers are looking for effective ways to quickly move from testing to production. However, in survey after survey, security and complexity of integration remain the two primary deployment bottlenecks," said Josh Jabs, vice president, office of the CTO and GM IIoT solutions for Entrust Datacard. "By integrating ioTrust into the ADLINK solutions and aligning deployment options with the customer test and build processes, we've removed these barriers thus enabling customers to securely bring turnkey data analytics and automation to the edge."

Together, ADLINK and Entrust Datacard will control the flow of data between applications, in the cloud and on the edge of IIoT environments. The partnership will also enable secure communication for data streams at the edge – while at rest, in motion and in use – with an enhanced level of granularity not seen in other solutions. Furthermore, this level of specificity will allow customers to control, monitor and even monetize unique data streams.

"Our Digital Experiment as-a-Service offering is helping organizations test and assess one or multiple business hypotheses based on the impact of an IIoT solution," said Lawrence Ross, General Manager Software and Solutions. "The integration of ioTrust's unique security capabilities and technology-agnostic design with DXS, means we're able to provide our customers with an even more secure solution for their IIoT-based endeavors, whilst also creating a process for turnkey data analytics at the edge. The integrated solution allows customers to complete use-case validation and quickly transition to a secure production environment."

Entrust Datacard and ADLINK will be present at the IIoT Solutions World Congress in Barcelona from October 16-18 demonstrating secure by design Edge IIoT – Please find us in Hall 2, inside the Industrial Internet Consortium's pavilion, Stand # D411.

For more information on Entrust Datacard and the ioTrust™ Security Solution, visit www.entrustdatacard.com/internet-of-things/.

To learn more about ADLINK Digital Experiments as-a-Service, visit https://www.adlinktech.com/Products/IoT_solutions/Vortex_Edge/DXS?lang=en

About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences – whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information, visit www.entrustdatacard.com.

These 5 IoT Energy-Harvesting Options Stand Out "in the Field"

As embedded systems and IoT devices push more into applications in remote locations, designers are looking at alternative means to portably power them.

[Cabe Atwell](#) | Jul 16, 2018 | Source [Electronic Design](#)

Thanks to advances in low power and energy efficiency, embedded systems and IoT devices no longer require access to ac current, meaning those platforms are suitable for remote applications. Wireless communication is becoming more prevalent in remote areas as well, opening the door to new operation possibilities like environmental sensor and telemetry applications, compiling weather data, and monitoring pipelines (among a host of others).

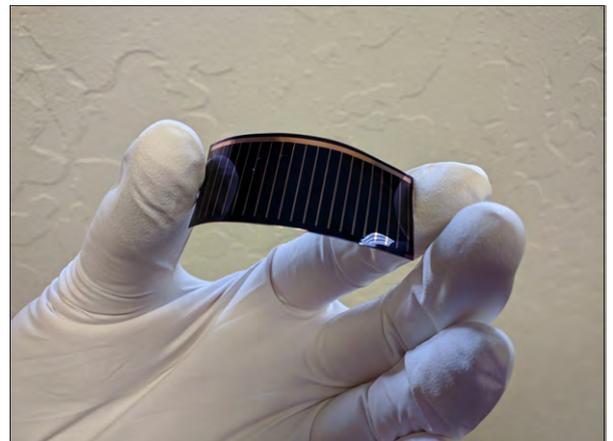
New [energy-harvesting technologies](#) coupled with energy-efficient battery storage and low-power platforms have pushed the boundaries of where embedded systems, IoT, and edge devices can be utilized. Whatever the application, all electronic devices require power of some sort, and energy harvesting is already allowing them to operate in a standalone manner, reducing managing costs and maintenance time in the field.

As it stands, a myriad of energy-harvesting devices can be paired with embedded systems and IoT devices capable of tapping into any number of resources—solar, thermal, wind, tide, kinetic, and many more. This roundup provides snapshots of some of the latest technologies that allow those devices to siphon energy from their surroundings for operation in remote areas.

Solar Energy

Solar power can provide an indefinite level of energy to IoT and embedded platforms as long as there's sunlight, but there are caveats—some cells are bulky and have low efficiency when it comes to energy conversion, especially for small devices. To get around those limitations, [Alta Devices](#) developed a single-junction flexible solar cell that has a 28.9% conversion rating from the [NREL](#).

The company's single-junction cell, based on gallium arsenide (GaAs), is flexible, lightweight, and thin, allowing it to be incorporated into small device designs with curved surfaces. The cell also packs Alta's [AnyLight](#) technology, which enables it to harvest light sources from both outdoors and indoors and convert it into an electrical current to recharge onboard batteries quickly and efficiently.

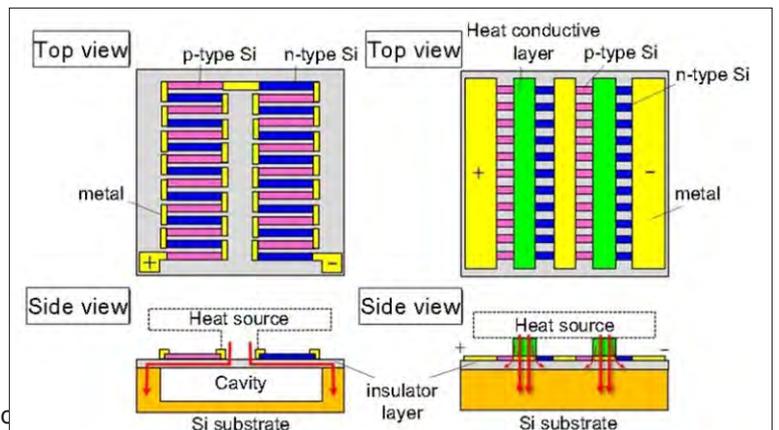


Alta Devices' single junction solar cell is GaAs-based and has an efficiency of 28.9%. (Image credit: Alta Devices)

Thermoelectric Energy

Researchers from Waseda, Osaka, and Shizuoka have designed a tiny [thermoelectric generator](#) that's capable of producing 12 μW per 1 cm^2 utilizing a small thermal difference of just 5°C. Their goal is to have it charge small autonomous IoT devices and embedded systems using environment or body heat.

The researchers state that their generator uses the same technology to manufacture semiconductor ICs. Usually, thermoelectric generators employ silicon nanowires at lengths of 10 to 100 nm that are suspended over a cavity; a heat current flows through to harness the temperature differential. The problem with that design is it weakens the mechanical strength so they shorten those nanowires to 0.25 nm, which allows them to maintain strength and minimize the generator while maintaining power density.



[Waseda Universities](#)' high-power thermoelectric generator can produce energy with a temp differential of just 5°C. (Image credit: Waseda University)

... to next page

These 5 IoT Energy-Harvesting Options Stand Out “in the Field”

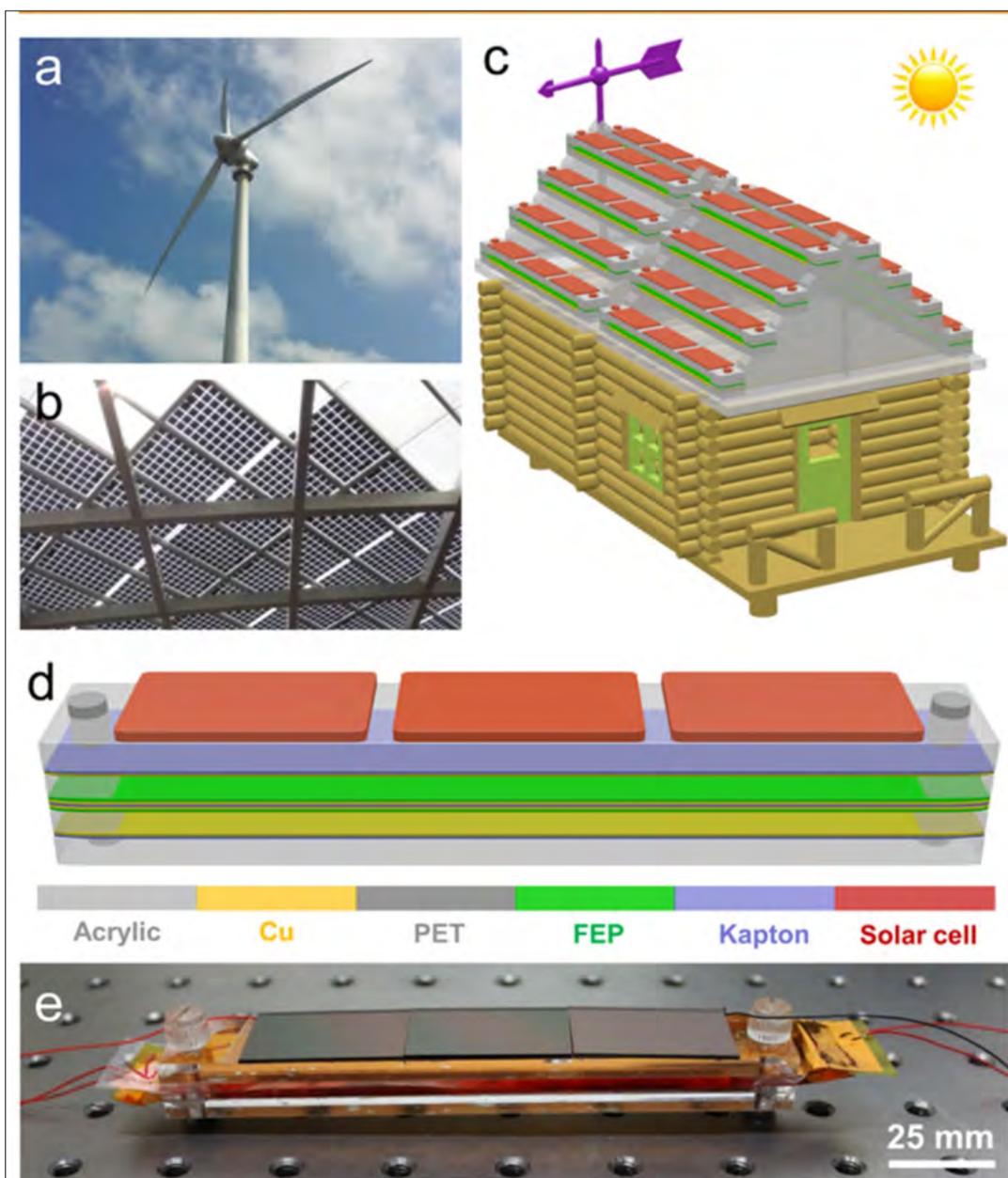
... from previous page

Wind Energy with a Side of Solar

Scientists from the [National Center for Nanoscience and Technology](#) (Beijing) have designed a device that's able to harvest solar and wind energy on a single platform.

The Hybridized Nanogenerator is aimed at supplying renewable energy to smart cities, but can be utilized for embedded systems and IoT devices.

The device integrates a highly efficient solar cell with a triboelectric nanogenerator that can convert wind energy into electrical output. On the solar cell side, the component is able to produce 8 mW of power, while the wind harvester can deliver up to 26 mW—a significant feat, since the platform only measures only 120 × 22 × 2 mm.



Illustrated is the National Center for Nanoscience and Technology's hybrid solar and wind harvesting cell.
(Image credit: NCNT via ACS)

... to next page

These 5 IoT Energy-Harvesting Options Stand Out “in the Field”

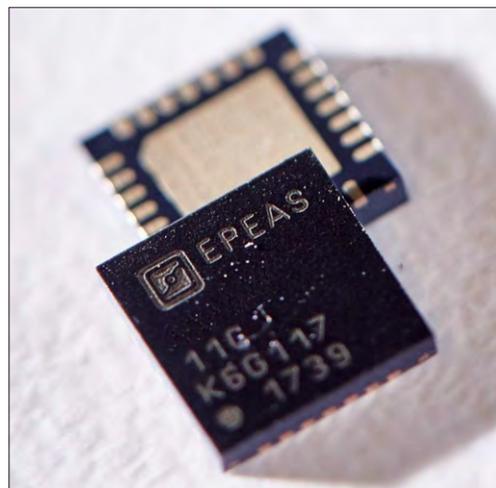
... from previous page

RF Energy

When it comes to harvesting RF energy with a tiny footprint, the [E-peas AEM40904 PMIC](#) takes the cake. The company's 5- × 5-mm RF power-management IC (PMIC) features a boost converter with a 94% efficiency that integrates voltage references, energy-management options, and low-dropout (LDO) regulators (1.2/1.8 V and 1.8/3.3 V).

It supports ultra-low-power startup (380 mV/3 μW) and features an RF input power from -18.5 dBm up to 10 dBm.

The harvested energy can simultaneously power embedded or IoT systems at 1.8 V while storing excess energy in several storage options, including lithium-polymer (LiPo) and thin-film batteries as well as capacitors and supercapacitors. What's more, you can use two batteries or storage devices and automatically switch from the secondary battery to the primary when the energy is depleted. What's great about this PMIC is it can be utilized with nearly any SoC or microcontroller with embedded systems or IoT applications.



The E-peas AEM40940 PMIC can harvest RF input currents up to 125 mA and store the energy in batteries or capacitors. (Image credit: E-peas via Fujitsu)

Vibration Energy

Staying on the PMIC trend, [Cypress Semiconductor](#) will be releasing its [CY39C811](#) device (still in production)—an ultra-low-power buck converter that features dual energy inputs capable of harvesting solar and vibration energy. Like the E-peas PMIC, this too can be used with just about any SoC or microcontroller, opening up many options for field-based IoT or embedded-system projects.

Key features the CY39C811 include an integrated low-loss full-wave bridge rectifier, a input voltage range of 2.6 to 23 V (with eight presets to choose from), an output current of up to 100 mA, overcurrent limit protection, I/O power-good detection signal output, and more.

Both market-ready and in-development technologies to power IoT devices and embedded systems go beyond utilizing battery-only platforms. All of those harvesters act as power generators for those rechargeable batteries or capacitors, which have become efficient in their own right. Coupling them together allows for off-grid applications where maintenance and data collection are performed in months rather than in days or weeks.



Cypress's CY39C811 PMIC features dual inputs, capable of harvesting vibration and solar energy. (Image credit: Cypress)

The future will see improved energy-collection technology where energy storage is the mitigating factor, rather than the actual harvesters. The most promising advances in portable power will encompass wireless-power transfer tech, along with improvements in solar, mechanical, and thermoelectric harvesting platforms. An increase in smaller, more efficient PMICs are due down the pipeline, along with low-power MCUs, empowering both the IoT and embedded-system fronts.

Fundamentals of Power

Welcome to the Power Design Center.

Here you will find resources, tips and tools that will help you with your power design decisions by market, product type, and topology. This hub will be your key reference center whether you are a new or seasoned power engineer.

[Over 25 applications notes FREE for direct download](#)

